

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

UNITED STATES OF AMERICA,

v.

CHARLIE JAVICE and OLIVIER AMAR,

Defendants.

23-cr-00251-AKH

**REPLY IN SUPPORT OF DEFENDANT OLIVIER AMAR'S
MOTION TO SUPPRESS GOOGLE DRIVE MATERIALS**

TABLE OF CONTENTS

PRELIMINARY STATEMENT	1
ARGUMENT	2
I. The Government's Google Drive Searches Violated the Fourth Amendment	2
II. Mr. Amar Has a Privacy Interest in His Google Drive.....	5
CONCLUSION.....	8

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>In re Asia Global Crossing, Ltd.</i> , 322 B.R. 247 (Bankr. S.D.N.Y. 2005).....	6
<i>In re Reserve Fund Securities & Derivative Litigation</i> , 275 F.R.D. 154 (S.D.N.Y. 2011).....	6, 7
<i>United States v. Almaleh</i> , 2022 WL 602069 (S.D.N.Y. Feb. 28, 2022).....	4
<i>United States v. Chuang</i> , 897 F.2d 646 (2d Cir. 1990).....	5–6
<i>United States v. Clark</i> , 638 F.3d 89 (2d Cir. 2011).....	3
<i>United States v. England</i> , 2019 WL 9633210 (E.D. Ky. Dec. 11, 2019).....	7
<i>United States v. Metter</i> , 860 F. Supp. 2d 205 (E.D.N.Y. 2012)	6
<i>United States v. Nejad</i> , 436 F. Supp. 3d 707 (S.D.N.Y. 2020).....	4
<i>United States v. Nejad</i> , 487 F. Supp. 3d. 206 (S.D.N.Y. 2020).....	5
<i>United States v. Sosa</i> , 379 F. Supp. 3d 217 (S.D.N.Y. 2019).....	4
<i>United States v. Wey</i> , 256 F. Supp. 3d 355 (S.D.N.Y. 2017).....	6
<i>United States v. Zemlyansky</i> , 945 F. Supp. 2d 438 (S.D.N.Y. 2013).....	3

PRELIMINARY STATEMENT

Before this Court is one simple question: did the Government search materials without the proper authorization to do so. The record is clear that the answer is yes. Despite the Government's mental gymnastics, the issue here boils down to one inescapable conclusion—the Government once again knowingly and intentionally has violated the Fourth Amendment rights of a defendant. Either the Government violated the Fourth Amendment by searching materials deemed nonresponsive under the search warrant or it violated the Fourth Amendment through an unreasonably lengthy review of Mr. Amar's Google Drive. The Supreme Court has held that suppression is warranted where needed as a prophylactic measure to deter bad conduct by law enforcement—this case demonstrates the need for such deterrence.

The Government continues to refuse to answer key questions about its review, and that refusal is telling. When, and how, and pursuant to what authority it claims to have identified responsive documents from Mr. Amar's Google Drive remain unanswered and must be answered to evaluate the scope of the violation here and the appropriate remedial measures. At the very least, these significant issues require the Government to adduce evidence in the form of affidavits or an evidentiary hearing.

That the gravamen of the Government's opposition is whether Mr. Amar has standing to bring these claims is as telling as it is misguided. As the Government well knows—demonstrated at least by the fact that it had to obtain a search warrant for Google without the consent of JP Morgan ("JPMC" or the "Bank") and that it decided to produce each Defendant's Google Drive solely to each individual defendant—Mr. Amar had a clear expectation of privacy in the materials they obtained and ultimately illegally searched. The Court should reject the Government's attempt to shift attention for what it is: an acknowledgement that they did wrong. The Government cannot

be allowed to sweep a constitutional violation under the rug with an unsupported and implausible claim of an ongoing review and a standing argument that ignores the established factual test for an expectation of privacy. This U.S. Attorney’s Office repeatedly has been warned not to do what they have done here, and, rather than admit fault, the Government now has tripled down on its violation.

That constitutional violation cannot be swept aside by the Government’s refusal to engage on the issue. Mr. Amar’s Fourth Amendment rights were violated by the Government’s searches of his Google Drive; the Google Drive materials and all fruits derived therefrom must be suppressed.

ARGUMENT

The Government asks this Court to countenance the digital equivalent of conducting a search of an apartment, posting an FBI agent outside the apartment for eight months, claiming the search was “ongoing” and not “closed” due to the presence of the FBI agent, then re-entering the premises to search again eight months later. The fact that a Google drive instead of an apartment is at issue does not make the Fourth Amendment violation any more palatable. The Opposition’s indignation at Mr. Amar’s claims is neither righteous nor just. Despite repeated opportunities—including in the Opposition brief itself—and requests from Defendants, the Government fails to put forth a single fact that would support the claim that its review was ongoing. Those facts, if they exist, are squarely within the knowledge of the Government, and it should be required to present them in something other than the *ipse dixit* of a brief.

I. The Government’s Google Drive Searches Violated the Fourth Amendment

The Government inappropriately seeks to fault Mr. Amar for “speculation” “without a shred of evidence,” in bringing this motion. Gov’t Opp. (“Opp.”) at 4, 22, Dkt. No. 246. Despite

ample opportunity to do so (including the many attempts from Defendants to seek this information), the Government continues to refuse to provide any facts supporting its specious assertion that its review was ongoing through January 2025. Notably, that is nearly three months after the date this case was set for trial. Putting that aside, the Government very easily could clarify the scope of this issue, if not put it to rest, by providing a detailed chronology demonstrating their ongoing review from April 2024 through their subsequent production in December 2024. Their refusal to do so speaks volumes.

With no facts supporting the Government's claim that its review was ongoing, that claim should not be credited under the circumstances here: a substantial Google Drive production only three months after the review began and then a full eight months before the next Google Drive production, which fell almost two months after the original trial date and the day after the Government identified as trial exhibits nearly all of the documents produced. The much more likely conclusion is that the Government returned to materials it had deemed nonresponsive under the search warrant, conduct that the Government does not defend in its Opposition, as it is undeniably a violation of the Fourth Amendment.

Rather than clarify precisely what occurred in the lengthy stretch between its April 2024 and December 2024 productions, the Government falls back on its refrain of good faith and its new position that it will use only six documents from Google Drive at trial.¹ But again here the Government uses sleight of hand; its claim that "half" of those documents were produced in April 2024 is technically true but fails to disclose that the documents produced in April 2024 were only the metadata (which indicates who had access to the documents and when edits were made) and

¹ The Government's protests of good faith would fail in any event, as it has failed to provide any evidentiary support of that good faith, and it squarely bears the burden to do so. *See, e.g., United States v. Clark*, 638 F.3d 89, 100 (2d Cir. 2011); *United States v. Zemlyansky*, 945 F. Supp. 2d 438, 474 n.16 (S.D.N.Y. 2013).

critically not the substantive documents themselves, which were produced *for the first time* in December 2024. The Government further claims that because these exhibits were identified as relevant in May 2024, that proves their search continued through January 2025—with no further information on what occurred during those intervening eight months. And the Government continues to refuse to identify when the 13,000 documents produced in January 2025—three months after the initial trial date—were marked responsive, instead abandoning those documents. To credit the Government’s assertion of ongoing review in light of these actions would permit any prosecutor in the country to skirt the Fourth Amendment with the unsupported assertion that their review is “ongoing.”

But even if the Government’s search actually was ongoing through January 2025, that search cannot be reasonable. That there is no bright line rule on reasonableness does not give the Government carte blanche to claim indefinite ongoing review. Nor do the Government’s cited cases actually support the reasonableness of the purported review here. For example, in *United States v. Aguilar*, the government provided Defendants and the court with details regarding its search, including that the documents at issue were in two languages and involved several hurdles, such as nearly 10,000 non-searchable documents. *Aguilar*, 20 Cr. 390, Dkt. 160 at 7 (E.D.N.Y. July 7, 2023). And the cases cited in *Aguilar* likewise do not support the Government’s actions here—in *United States v. Sosa*, the court found a lengthy review that concluded nearly three months before trial reasonable. *Sosa*, 379 F. Supp. 3d 217, 222 (S.D.N.Y. 2019). The Government’s review here concluded less than three weeks before trial, and nearly three months *after* the original trial date. *United States v. Nejad* involved documents in three languages, and the Government neatly sidesteps Judge Nathan’s later opinion in that case. *Nejad*, 436 F. Supp. 3d 707, 735 (S.D.N.Y. 2020); *see Nejad*, 487 F. Supp. 3d. 206, 210 (S.D.N.Y. 2020). Finally, *United*

States v. Almaleh involved rolling productions of materials from 35 devices. *Almaleh*, 2022 WL 602069, at *20 (S.D.N.Y. Feb. 28, 2022). A production after three months of review and then another production eight months later, after the original trial date and Government's exhibit list deadline, are hardly rolling productions, not to mention the three Google Drives at issue here are a much smaller volume to review than 35 devices.

In sum, the Government violated the Fourth Amendment either through its return to materials deemed nonresponsive under the search warrant or in conducting an unreasonably lengthy search of Mr. Amar's Google Drive. The repetition of this Fourth Amendment violation by prosecutors specifically in this District, in the face of serious admonitions by the courts, makes plain that the only way to effectively deter this conduct from continuing is to suppress the Google Drive materials. Any other outcome would reinforce that prosecutors in this Office, or indeed nationwide, may blatantly violate the Constitution so long as they say the magic words "ongoing review" and refuse to provide factual support for that claim.

II. Mr. Amar Has a Privacy Interest in His Google Drive

The Government's misplaced focus on standing fails from both a legal and practical perspective. The touchpoint of standing to enforce the Fourth Amendment is the expectation of privacy, not the actual ability to enforce it. Otherwise, no one would have a privacy interest in their Google accounts, which ultimately are maintained by Google.² Mr. Amar had that expectation of privacy in his Frank Google account.

The Government attempts to establish a bright line rule whereby no employee can have a privacy interest in his work electronic accounts, but their own cases indicate that such a rule does

² This is further illustrated by Congress's enactment of the Stored Communications Act to further protect individuals' constitutional rights in their electronic communications, given the unique nature of the physical control of those accounts by third parties.

not exist. *See United States v. Chuang*, 897 F.2d 646, 649 (2d Cir. 1990) (“It is well-settled that a corporate officer or employee in certain circumstances may assert a reasonable expectation of privacy in his corporate office, and may have standing with respect to searches of corporate premises and records.”). While the court found the defendant had no privacy interest in the seized materials in *Chuang*, the Government conveniently neglects to mention that those materials were physical materials seized from the office of a different person—and even there the court observed that Chuang did have a legitimate expectation of privacy “in his own office.” *Id.* at 650. Indeed, courts in this Circuit have suppressed materials taken from defendants’ corporate offices, including electronic data from corporate email accounts. *See, e.g., United States v. Wey*, 256 F. Supp. 3d 355, 379 n.4, 410–11 (S.D.N.Y. 2017) (suppressing materials, including electronic data and hard drives, obtained from execution of search warrant at office of a private equity fund of which the defendant was the founder and principal executive); *United States v. Metter*, 860 F. Supp. 2d 205, 216 (E.D.N.Y. 2012) (suppressing electronic data seized from computer hard drives and email accounts seized from execution of search warrant at defendant’s office).

Instead, a “highly fact-specific” analysis is required, and cases largely turn on “the particular policy language adopted by the employer.” *In re Rsrv. Fund Sec. & Derivative Litig.*, 275 F.R.D. 154, 160 (S.D.N.Y. 2011). The relevant factors in determining an employee’s expectation of privacy in their use of company technology are widely accepted to be: “(1) does the corporation maintain a policy banning personal or other objectionable use, (2) does the company monitor the use of the employee’s computer or e-mail, (3) do third parties have a right of access to the computer or e-mails, and (4) did the corporation notify the employee, or was the employee aware, of the use and monitoring policies?” *Id.* (quoting *In re Asia Glob. Crossing, Ltd.*, 322 B.R. 247, 257 (Bankr. S.D.N.Y. 2005)). Because Frank’s policy did not ban personal use

and provided for limited, specific monitoring, Mr. Amar had a policy interest in his Frank Google account, including Google Drive.

Frank's electronic device and account policy provided that "the Employee will use the Company's assets and equipment (including the Laptop, Cellular Phone, email account assigned to it by the Company...) primarily for the purpose of his/her employment." Ex. A, Amar Personal Employment Agreement, 8.3. That employees were to use their accounts "primarily" for work contemplates that they may also be used for personal matters, far from a ban. The policy further provided that the Company had the right to conduct inspections only "upon reasonable suspicion of a breach of the provisions of this [Employment] Agreement or applicable law" and employees had to "transfer to the Company" their passwords. *Id.* at 8.4. In essence, Mr. Amar's Google account, including Google Drive, was akin to an adult son residing in a regularly locked room in his parents' home, where his parents do not enter his room without permission or upon suspicion of illegal activity; the son maintains a privacy interest in his room independent of his parents' interest in the overall home. Thus, Mr. Amar had a reasonable expectation of privacy in his use of his Frank Google account. *See In re Rsrv. Fund*, 275 F.R.D. at 160; *United States v. England*, 2019 WL 9633210, at *13 (E.D. Ky. Dec. 11, 2019) (holding that Defendant had an expectation of privacy in his company laptop where there was no policy against personal use, no employee had been disciplined for personal use of company computers, and Defendant used a password to lock the computer, even though employees understood that their employer had the ability to control their computers).

What is more, the Government's claim that Mr. Amar lacks a privacy interest in his Google Drive is belied by the Government's production of his full Google Drive to him alone, and of Ms. Javice's full Google Drive to her alone, in October 2023. Those separate productions illustrate the

Government's belief that each defendant did have a privacy interest in their own Google Drive. The Government also makes much of the fact that JPMC acquired the rights to Frank's Google accounts and was a highly regulated entity. But the Google Drive in question was tied to Mr. Amar's *Frank* account, and his use predated JPMC's acquisition of Frank. To overwrite his prior expectation of privacy at the time he used the Google Drive through a later acquisition is nonsensical. And from a practical perspective, if JPMC holds the privacy interest, it begs the question of why the Government needed to pursue a search warrant for the Google accounts at all rather than have JPMC—which was actively working with the Government—request the materials from Google. Or why, if a search warrant was a preferable process, the affidavit in support of the search warrant does not indicate that JPMC consented to the provision of the materials.

As Mr. Amar had a reasonable expectation of privacy in his Frank Google account, and the Government violated the Fourth Amendment in its searches of that Google Drive account, whether by impermissibly continuing to return to materials after the execution of the search warrant or by conducting an unreasonable search, the Google Drive materials must be suppressed to serve as a deterrent against similar conduct in the future. Absent court action, given the pattern of violations over the past several years, this conduct bears a high risk of recurrence.

CONCLUSION

For the foregoing reasons, the Court should suppress the materials obtained from Mr. Amar's Google Drive pursuant to the Google search warrant.

Dated: February 3, 2025

Respectfully submitted,

KOBRE & KIM LLP

/s/Sean S. Buckley

Sean S. Buckley
Jonathan D. Cogan
Alexandria E. Swette
Daisy Joo
800 Third Ave.
New York, NY 10022
Tel: (212) 488-1200
Sean.Buckley@kobrekim.com
Jonathan.Cogan@kobrekim.com
Alexandria.Swette@kobrekim.com
Daisy.Joo@kobrekim.com

Matthew I. Menchel
201 South Biscayne Boulevard
Suite 1900
Miami, FL 33131
Tel: (305) 967-6100
Matthew.Menchel@kobrekim.com

Erika L. Berman (pro hac vice forthcoming)
1919 M Street, NW
Washington, DC 20036
Tel: (202) 664-1900
Erika.Berman@kobrekim.com

Counsel for Defendant Olivier Amar